네트워크 보안 관리를 위한 계층적 위임 모델

이강희°, 송병욱, 배현철, 김장하, 김상욱
경북대학교 컴퓨터과학과
{khlee°, bwsong, hcbae, jhkim, swkim}@cs.knu.ac.kr

Hierarchical Delegation Model for Network Security Management

Kanghee Lee°, Byungwook Song, Hyunchul Bae, Jangha Kim, Sangwook Kim
Department of Computer Science, Kyungpook National University

요 약

본 논문에서는 대규모 네트워크 보안관리를 위한 계층적인 위임 모델을 제시한다. 대규모 네트워크는 라우터, 방화벽, 침입 탐지 시스템, 웹 서버 등의 수많은 구성요소로 이루어진 네트워크들의 집합이며, 각 네트워크마다의 독립적인 지역 정책들로 관리되어 서로간의 협동이 이루어질 수 없기 때문에 이를 효과적으로 통제하고 일괄적으로 관리하기 위해 계층적인 위임 모델이 사용되어야 한다. 제시하는 모델의 중요 구성 요소로는 관리 서버, 정책 설정 고 수준 언어, 고 수준 언어 컴파일러, 도메인 서버, 인터프리터, 정책 관리 데이터베이스가 있다. 관리 서버에서 정책 설정 고 수준 언어를 사용하여 세밀하고 정교한 정책을 작성할 수 있고, 이 정책을 고 수준 언어 컴파일러를 통하여 최하위 노드들에게 적절하고 간결한 형태로 만들어낸다. 각 도메인 서버는 이 결과를 하위의 도메인 서버나 인터프리터에게 전달하면서 Keynote 신뢰 관리 시스템을 이용하여 권한을 위임한다. 그리고 인터프리터는 정책을 라우터, 방화벽, 웹 서버 등의 하위 노드에 맞는 실제 룰로 변환하여 상위 관리 서버에서 전달한 정책을 적용하게 된다. 정책을 적용한 결과를 상위로 전달하여 데이터베이스를 구축한 뒤 후에 작성된 정책이 기존의 정책과 충돌하는지 검사에 이용하고, 충돌한다면 협상 과정을 거쳐 정책에 순응할 수 있는 결과를 도출하게 된다. 또한 네트워크에서 많은 새로운 형태들의 노드가 추가될 수 있는데, 각각의 인터프리터만 추가함으로서 다양한 하위 노드를 충족시킬 수 있는 확장성을 제공한다.

1. 서 론

대규모 네트워크는 넓은 영역에 걸쳐 한 네트워크와 인접한 각 네트워크를 모두 연결한 통신 네트워크이다. 이는 여러 종류의 형태를 가진 노드로 구성된 네트워크로 이루어진다. 또한 물리적으로도 멀리 떨어져 있고, 이들에 대한 관리는 분산적으로 이루어질 수밖에 없다. 만약 관리가 된다고 해도 네트워크를 구성하는 장비 또는 시스템의 수가 많고 규모가 크므로 정확한 세부 정보를 파악하기 어렵다. 그리고 네트워크의 구성, 구성 요소의 변동이 심하며 각 요소의 종류가 워낙 다양하기 때문에 공통적인 방식으로 접근하기 어려움이 있다. 따라서 기존의 관리 방식과 도구로는 효과적인 결과를 기대할 수 없다. 이러한 어려움을 생각해 볼 때 대규모 네트워크의 보안 관리 모델은 다음과 같은 몇 가지 문제를 해결할 수 있어야 한다. 첫째, 최상위에서 일괄적인 관리가 이루어질 수 있어야 한다. 따라서 계층적인 구조를 이루어야한다. 둘째, 계층적인 구조를 이루되 로컬 도메인의 자체적인 정책을 수용할 수 있어야 한다. 최상위의 관리 서버에서 한 정책을 전달했지만 특정한 로컬 도메인의 자체 정책과 충돌이 일어난다면 이를 적절히 협상할 수 있는 메커니즘이 필요하다. 셋째, 계층적인 구조를 사용하기 위해서는 인증과 권한에 관한 부분이 먼저 해결되어야 한다. 넷째, 최하위 노드의 공통적인 특징을 표현할 수 있는 형식이 있어야 한다. 이들 요소는 일반적인 공통된 역할과 각자의 특수한 기능을 내포한다. 일괄적인 관리를 위해서는 각각의 기능을 아우를 수 있는 형식이 필요하며, 본 논문에서는 Common Access Management Form(이하 CAMF)를 정의하여 사용한다. 마지막으로 CAMF 같은 공통적인 기능을 간추린 형식을 가지고 실제의 하위 노드의 형식으로 변환하는 메커니즘과 도구가 필요하다. 네트워크 보안 관리를 위한 계층적 위임 모델의 구성 요소 중 인터프리터가 이 역할을 담당하게 된다. 예를 들어 특정 모델의 라우터를 담당하는 인터프리터가 CAMF를 실제 라우터의 명령어로 변환하는 작업을 담당하게 된다.

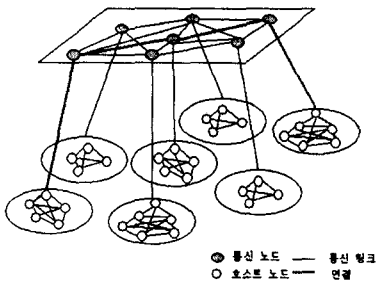
대규모 네트워크를 안전하게 관리하기 위해서는 앞서 말한 문제점을 해결함과 동시에 이질적인 노드를 효율적으로 관리하고 또한 구성 요소들 간의 협동 및 유기적인 관계를 지원하는 보안 관리 구조가 필요하다. 이 구조를 효과적으로 이용하기 위해서는 자동화된 관리 메커니즘이 요구되며, 이 메커니즘으로 네트워크 구성 요소에 제어와 통제가 이루어지기 위해서는 각 노드의 세부 정보를 관리하는 데이터베이스가 필수적이다. 대규모 네트워크의 구성을 2장에서, 네트워크 보안 관리를 위한 위임 모델을 3장에서 설명하고 4장에서는 결론을 맺는다.

2. 대규모 네트워크의 구성

2.1 구조 및 특징

대규모 네트워크는 넓은 영역에 걸쳐 각 네트워크를 모두 연결한 구조를 <그림 1> 과 같이 가진다. 여러 종류

의 호스트들과 라우터 및 스위치 등의 장치로 구성된 다양한 네트워크로 이루어지고 이들은 지리적으로 떨어져 있고, 관리 또한 소규모의 도메인 단위로 이루어지고 있다. ISP 업체와 IX를 기준으로 국내외로 연결되어 있다.



<그림 1> 네트워크 구조

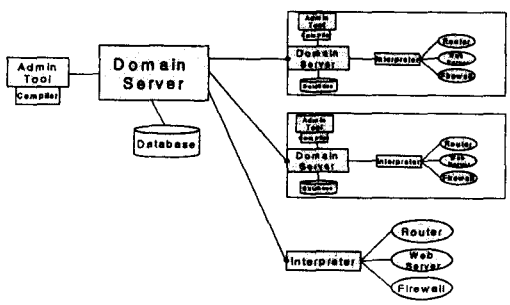
2.2 보안 취약성

대규모 네트워크는 다양한 종류의 많은 호스트와 장치, 하위의 네트워크로 구성되므로 다양한 취약점이 존재할 수 있다. 침입자의 입장에서는 이러한 취약점을 이용하여 대규모 네트워크를 효과적으로 공격할 수 있는 계기가 된다. 또한 대규모 네트워크가 지원하는 네트워크 운영체제의 모든 호스트들과 장치들은 독립적이고 모든 관리가 분산적으로 이루어지므로 대규모 네트워크를 대상으로 한 공격은 방어하기 어렵다. 그리고 현재 우리나라의 초고속 통신망은 다른 국가 간에 경유지로 악용됨으로서 바이러스나 인터넷 웜들의 유입과 크래커들의 공격을 많이 받고 있으며, 급속도로 발전된 네트워크에 비해 전문 관리인력 부족으로 인하여 보안에 취약한 점도 문제가 되고 있다.

3. 네트워크 보안 관리를 위한 위임 모델

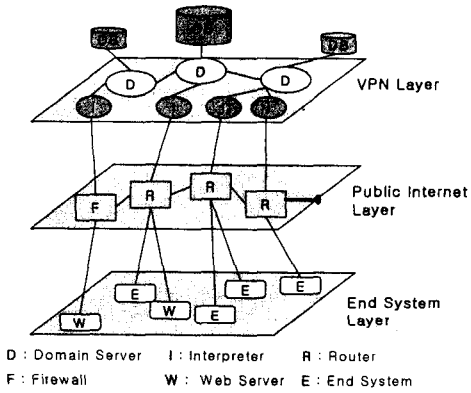
3.1 구조 및 특징

네트워크 보안 관리를 위한 계층적 위임 모델의 기본 구조는 <그림 2> 와 같다.



<그림 2> 계층적 위임 모델의 기본 구조

물리적으로는 떨어져 있을 수 있지만 보안 관리를 위해서 논리적인 하나의 트리로 구성되며 최상위 네트워크의 구조를 하위 네트워크들도 똑같이 가지게 된다. 각 네트워크의 도메인 서버는 자신의 상위와 하위의 도메인 서버들과 정책 적용 협상을 하고 권한을 위임하거나 받게 된다. 안정적인 관리가 이루어지려면 Private Network로 구성되어 모든 구성 요소들이 Public Network와는 구분되어야 한다. 하지만 현실적으로 Private Network를 구성하기에는 어려움이 많기 때문에 <그림 3> 과 같이 VPN을 구성하여 계층적인 위임 모델을 구성할 수도 있다.



<그림 3> VPN을 이용한 위임 모델

고 수준 언어로 작성된 정책을 시작으로 컴파일러가 CAMF의 형태로 도메인 서버들에게 전송해주고 인증 정보를 덧붙여 하위의 도메인 서버로 다시 전송하거나 자신이 관리하는 하부 노드의 인터프리터에게 정책을 전송하게 된다. 도메인 서버 혹은 인터프리터 간의 인증 정보는 다음과 같은 형태의 Keynote 신뢰 관리 시스템을 이용하게 된다.

```
Authorizer: "POLICY"
Licensees: "rsa-hex: 3048024100d15d08ce7d2103₩
        d93ef21a87330361ff123096b14₩
    330f9f0936e8f2064ef815ffdaab₩
    28558e10203010001"
Conditions: (command=="setting rule" ||
    command=="checking state") &&
    (app_domain=="knu.ac.kr")
Signature: "RSA-SHA1:3896567347348"
```

이와 같은 신뢰 관리 시스템에서는 authorizer에 대한 인증 뿐 아니라 어떤 조건을 통한 action에 대한 통제 권한도 인증하기 때문에 더욱 더 사용하기에 유용하다.

3.2 고 수준 정책 언어 및 컴파일러

고 수준 언어는 세부적으로 알 수 없는 네트워크를 일괄적으로 가장 효과적으로 조정하기 위한 것이다. 따라

서 다음과 같은 언어적, 형태적인 특징을 가져야한다.

1) 최대한 일반적인 형태에 가깝게 한다.
2) 네트워크 모델과 직관적인 연결이 가능하게 한다.
3) 관리 범위를 결정할 수 있다.
4) 관리를 통해 나타나는 결과를 결정할 수 있다.

아래는 위의 4가지 항목을 토대로 설계한 고 수준의 정책 설정 언어를 이용하여 간단한 네트워크 관리 정책을 표현한 예이다.

```
policy SamplePolicy {
        for( "knu.ac.kr" ) {
         incoming {
                if( src_addr == "155.230.1.1"
                   && protocol == "UDP" ) {
                      deny;
                }
         }
        }
}
```

일반적으로 사용하는 언어의 형태와 비슷하게 구성하고, incoming, outgoing, protocol 등의 변수를 사용하여 네트워크 모델과 직관적으로 연결하였다. 또한 "knu.ac.kr" 와 같은 적용되어질 도메인을 구분지어 관리의 범위를 결정지었다. 마지막으로 조건에 맞는 상황일 때에는 패킷을 차단하는 "deny" 와 같은 키워드를 사용할 수 있다. 이렇게 작성된 정책으로 네트워크 구성 요소의 정책을 쉽게 작성할 수 있게 된다. 위와 같은 형태로 작성된 정책을 컴파일러는 최종적으로 <표 1>의 CAMF 로 바꾸게 된다.

[표 1] CAMF의 예시

PolicyName	SamplePolicy
Domain	knu.ac.kr
Direction	incoming
Action	Deny
Src Address	"155.230.1.1"
Src Port	ALL
Dst Address	ALL
Dst Port	ALL
Protocol	UDP
Priority	10

3.3 도메인 서버 및 인터프리터

도메인 서버와 인터프리터는 상위에서 전달된 정책을 실제 노드에 적용시키는 중요한 구성 요소이다. 이 두 요소간의 통신은 CAMF 형태로 이루어지며 CAMF에는 기본적인 정책의 정보를 포함한 수행 결과나 데이터베이스에 대한 질의 정보도 함께 주고받게 된다. 여기에서 CAMF는 정책을 전달하기 위한 중간 형태의 언어 역할뿐만 아니라 통신을 위한 프로토콜의 형식을 띠게 된다.

먼저 도메인 서버는 정책을 수신, 가공, 분배, 결과 기록 하는 역할을 담당한다. 국지적인 네트워크의 관리는 해당 도메인 서버가 전담하게 되고 전체를 관리하는 상위의 도메인 서버의 정책과는 충분히 협상할 수 있는 메커니즘이 구현된 모듈이 존재하게 된다. 이 협상 메커니즘은 기존의 정책 설정 정보 등을 데이터베이스를 통해 얻게 된다.

인터프리터는 최하위의 다양한 노드들과 직접적으로 통신하는 구성 요소이다. 따라서 ToolKit 의 형태로 구성된다면 새로운 형태의 하부 노드가 추가된다 하더라도 쉽게 인터프리터 형태를 작성할 수 있고, 추가된 하부 노드에 맞는 언어적인 형태를 분석하여 번역하는 모듈을 작성하여 통합하면 된다. 정책의 충돌 협상과 같은 작업은 상위의 도메인 서버의 협상 메커니즘에서 처리하므로 인터프리터는 단지 수신 받은 정책을 적용하고 그 결과를 모두 상위의 도메인 서버에게로 전달해주는 작업을 하면 된다.

4. 결론

본 논문에서는 대규모 네트워크를 구성하는 노드들의 특징을 기반으로 발생하는 보안관리의 문제점을 분석하고 이를 극복하기 위한 계층적인 위임 모델을 정리하였다. 또한 Keynote 신뢰 관리 시스템을 이용하여 보안 관리 구조를 설계하였으며 고 수준 정책 언어에서 도메인 서버, 인터프리터로 이어지는 계층적인 모델은 다양한 하위 노드들에 대한 확장성을 지원한다. 대규모 네트워크에서는 각각의 구성 요소들이 결합된 자동화 된 메커니즘 없이는 보안 관리가 이루어지기 어렵기 때문에 본 논문의 모델이 더욱 더 연구되어야 할 것이며 향후에는 다양한 네트워크 구성 요소에 적용할 수 있는 고 수준 언어의 확장과 보다 많은 시스템 정보를 수집하여 정책의 적용 부분 중 협상 과정에 대한 문제점을 해결하는 연구를 진행할 것이다.

[참고 문헌]

[1] Dynamic Coalitions, http://www.iaands.org/iaands2002/dc/

[2] Hoagland, J.A., Pandey, "Security Policy Specification Using a Gra phical Approach," Technical Report CSE-98-3, U.C.Davis, 1998.

[3] Lobo,J., R.Bhatia "A Policy Description Language," AAAI, 1999.8] Nicodemos Damianou, "The Ponder Policy Specification Language", Proc. of Workshop on Policies for Distributed Systems and Networks, Jan. 2001

[4] N. Dulay,E. Lupu, M. Sloman, N. Damianou, "A policy deployment model for the Ponder language," Integrated Network Management Proceedings, 2001 IEEE/IFIP International Symposium on, 14-18 May 2001

[5] J.Levine, "Lex & Yacc", O'Reilly, 2001

[6] Cisco Assure QoS Policy Manager http://www.cisco.com/warp/public/cc/pd/nemnsw/cap